METHOD AND SYSTEM FOR AUTHENTICATED ACCESS TO INTERNET PROTOCOL (IP) MULTICAST TRAFFIC

TECHNICAL FIELD OF THE INVENTION

This invention relates generally to the field of traffic multicasting, and more particularly to a method and system for authenticated access to Internet protocol (IP) multicast traffic.

BACKGROUND OF THE INVENTION

Internet protocol (IP) multicast is an Internet standard that enables bandwidth-efficient distribution of video, audio and other data through a network. IP multicast packets are addressed to a group address rather than to a destination IP address such as in a traditional point-to-point communication. The network path that such packets take as they are routed through the network forms a distribution tree.

At the edge of the network, traffic for a multicast group is discarded unless one or more local user devices have joined the group. A user device joins the group by issuing a join request which is automatically processed by the edge device. The edge device then forwards multicast traffic for the group to the user.

The advantage of IP multicast is that even when there are multiple users interested in receiving the same data, only a single copy of the data travels through the backbone network to the network edge. At the edge, the date is replicated and separately transmitted to the users.

IP multicast, however, is geared toward enterprise or corporate networks that permit anyone to join a multicast group. Thus, any user on the network is able to receive multicast traffic as long as that data is available on the network. As a result, service provider networks cannot use IP multicast to distribute premium services.

SUMMARY OF THE INVENTION

The present invention provides a method and system for authenticated access to Internet protocol (IP) multicast traffic that substantially reduce or eliminate problems and disadvantages associated with previous systems and methods. In a particular embodiment, the present invention authenticates access privilege of users attempting to join multicast groups to enable service providers to provide controlled access to value-added services based on multicast content such as video and audio.

In accordance with one embodiment of the present invention, a method and system for authenticated access to multicast traffic receives a request for a user to join a multicast channel. Access privileges of the user to the multicast channel are authenticated. The request is disallowed in response to at least an unsuccessful authentication.

More specifically, in accordance with a particular embodiment of the present invention, the request is allowed in response to at least successful authentication. Authentication of access privileges may be based on the type of the multicast channel, the type of the request to join the multicast channel, or the logged in status of the user to a service provider and/or service including the multicast channel.

The technical advantages of the present invention include providing a method and system for authenticated access to IP multicast traffic. In a particular embodiment, a user request to join a multicast channel is intercepted in an access router and the access privileges for the user authenticated using previously provisioned

user access information. Depending on the success of authentication, the join request is allowed or disallowed. Accordingly, users can only join multicast channels that are public or to which they have subscribed and service providers may provide value-added services efficiently over the network using IP multicast.

Another technical advantage of one or more embodiments of the present invention includes providing an improved network-based content delivery system. In particular, service providers are able to distribute content over a network in access-controlled multicast channels. This enables subscription-based business models where service providers can bundle different multicast streams into packages of content to which users can subscribe. As a result, service providers are provided with a new range of revenue opportunities.

Still another technical advantage of one or more embodiments of the present invention includes providing an improved method and system for differentiating services for users sharing common equipment. In particular, different users are allowed access to different multicast video and audio content based on user identification rather than device identification. For example, a parent can subscribe to content different than a child in a same residence.

Other technical advantages of the present invention will be readily apparent to one skilled in the art from the following figures, description and claims.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and its advantages, reference is now made to the following description taken in conjunction with the accompanying drawings, wherein like numerals represent like parts, in which:

FIGURE 1 is a block diagram illustrating a communication system including video multicast services in accordance with one embodiment of the present invention;

FIGURE 2 is a block diagram illustrating details of the multicast authentication components of the communication system of FIGURE 1 in accordance with one embodiment of the present invention; and

FIGURE 3 is a flow diagram illustrating a method for authenticated access to Internet protocol (IP) multicast traffic in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

FIGURE 1 illustrates a communication system 10 in accordance with one embodiment of the present invention. In this embodiment, service and/or content providers provide video services to users through multicast channels to which access is controlled to allow the providers to bill for premium content. Accordingly, some content such as basic network television channels will always be available to users free of charge, but content such as pay-per-view and premium channels are controlled to retain their value at a source of potential revenue. Other services such as Webcam, local, or other special interest group channels may be controlled for privacy and security reasons. Accordingly, service and other providers can deliver differentiated, community or other group-focused services with specific channels as part of a multicast service offering. In providing services, providers can employ content switching mechanisms to replace programming options. For example, a local news program can preempt or replace national programming. It will be understood that in addition to video, audio, data and/or combinations of content types may be provided to users through the access controlled multicast channels. Audio may be radio, music channels or audio-only training materials. Data content can be stock quotes, software distribution and the like.

Referring to FIGURE 1, the communications system 10 includes a content provider network 12, the Internet 14, a transport network 16, an access network 18 and end user systems 20. A satellite network 22 may overlay portions of the system 10. The content provider network 12, Internet 14, transport network 16, access network 18, end

user system 20, satellite network 22 as well as components of the networks and systems are connected by any suitable wireline or wireless links. In a particular embodiment, the network and systems communicate traffic in Internet protocol (IP) packets. In this embodiment, video services are provided through IP multicast channels. It will be understood that one or more of the networks or systems or portions of the networks or systems may communicate traffic using asynchronous transport mode (ATM), synchronous optical network (SONET) and/or other suitable protocols without departing from the scope of the present invention.

The content provider network 12 receives and/or locally generates video streams. Input video streams 36 are encoded for efficient transmission over the communications system 10 by codec 30 and persistently stored by content delivery server 32. Live content may be fed directly from the codec 30 over the communication system 10 for delivery to end users.

In the IP multicast embodiment, video content is typically encoded in the MPEG 2 format. For performance reasons, the IP packet size used for video streaming should be maximized because larger IP packets leads to a reduced number of packets for the same amount of data and thus reduce routing overhead. If ATM is utilized for transport of the packets, packet size should fit evenly into ATM cells.

The video streams may include broadcast television and cable channels such as bundled commercial channels, basic network television channels, premium channels, pay-per-view channels and public channels. The video streams may also include special interest group channels, local

channels, Webcam channels, e-learning channels, and local advertisement channels. The special interest group channels may be targeted at niche audiences having the potential for rapid growth. Local channels may spotlight local cultural events, sports, and other local activities. The Webcam content channels allow mobile users to visually monitor premises, such as homes or daycare centers and enable security agencies to enhance home video services. The e-learning channels enable online learning or education with video from training rooms. The local advertisement channels can be inserted by providers to gain incremental revenue.

The video streams may be transported from the content provider network 12 to an access network or other points of presence (PoP) for delivery to end users using the Internet 14, transport network 14, satellite network 22 or any other suitable network capable of multicasting traffic. Because streaming video over the Internet 14 does not provide quality of service (QoS) controls to a service provider, the end user experience may vary depending upon changes in the traffic load and the native intelligence and configurations of Internet devices along the route. Accordingly, the video streams may be delivered using the transport network 16 which provides a high-quality delivery in a "walled garden" environment enabling the provider to implement strong end-to-end controls over signal quality. Alternatively, the video streams may be transported over the satellite network 22 which may be private to content providers. The satellite network 22 includes a satellite transmitter 24 at the content provider network 12, one or more satellites 26 and a satellite receiver 28 at the access network 18.

The satellite network 22 conserves core bandwidth of the transport network 16 and makes the video quality independent of QoS configurations of the transport, or core network 16.

As described in more detail below, the video streams are transported between the content provider and access networks 12 and 18 using IP multicast. Accordingly, only one multicast video stream is transmitted to an access network 18, independently of the number of subscribers. The router nearest the subscriber dynamically, on demand from subscribers, replicates the multicast stream and forwards the replicated streams in the access network 18 to subscribers.

The transport network 16 is an intranet or other wide area network (WAN) capable of transporting video streams from the content provider network 12 to the access network 18. The transport network 16 is multicast enabled and transmits multicast packets in the form of a distribution tree between the content provider network 12 and access networks 18.

The transport network 16 is configured to support the aggregated bandwidth of each access network 18, or central office (CO) as well as high bandwidth multicast video content when video is transported over the core. In a particular embodiment, the transport network 16 comprises backbone routers 40 connected by OC-48 or OC-12 links and transports traffic in the packet over SONET (PoS) format.

The backbone routers 40 utilize protocol independent multicast (PIM V2) or other suitable multicast routing protocols. PIM operates in a dense mode, a sparse mode, or a sparse-dense mode. The sparse-dense mode enables a

hybrid environment that allows some heavily accessed channels to be configured in dense mode and others in sparse mode. It will be understood that other modes and/or multicast routing protocols may be used in the transport and other networks without departing from the scope of the present invention.

In a particular embodiment, the precedence of the IP packets is set to committed access rate (CAR) at content aggregation in the content network 12. CAR allows packets to be flagged and/or dropped if they maintain or exceed static bandwidth configurations and can be implemented with a simple configuration. The rate limiting capability of CAR can be optimally used to control the amount of bandwidth for IP multicast streams from the content provider network 12. In this embodiment, the transport network 40 may implement a weighted random early detection (WRED) protocol for congestion management and congestion avoidance. Weighted fair queuing (WFQ) may be used in the access network 18. WFQ breaks up the usable bandwidth based on the current precedence of the packets currently queued to allow for a statistically more balanced queue.

The transport network 16 is coupled to and/or includes a service selection dashboards (SSD) server 42 and an authentication, authorization, and accounting (AAA) server 44. The SSD server 42 provides users with logon pages for their service provider and subscribed services. The SSD server 42 also generates and provides users with web pages displaying options available for selections. For example, after a user has logged onto a service provider, the SSD server 42 may generate and

display to the user a web page including the services to which the user has subscribed and may select.

The AAA server 44 maintains user and service profiles. The profiles are stored persistently and accessed directly or indirectly to authenticate users and services for users. In one embodiment, the service profiles include a list of multicast IP addresses associated with each premium or other non-public service. As used herein, each means every one of at least a subset of identified items. The user profile correlates the user identity with subscribed service packages, and thus subscribed channels. In a specific embodiment, the AAA server 44 provides standard remote authentication dial-in user service (RADIUS) based functionality.

The access network 18 communicates traffic between the Internet, transport, satellite or other suitable core network and the end user system 20. In the illustrated embodiment, the access network 18 comprises an asymmetric digital subscriber line (ADSL) architecture to provide high downstream and low upstream bandwidth which is well-suited for delivery of multicast video services. The DSL access architecture may be point-to-point over ATM (PPPoA), point-to-point over Ethernet (PPoE), route bridge encapsulation (RBE) or other suitable architecture. It will be understood that symmetric, very-high speed and other DSL technologies may be used as well as other suitable access technologies for communicating between the core network and the end user system 20.

The access network 18 includes an access router 60 coupled to the core network and a plurality of digital subscriber line access multiplexers (DSLAM) 62 coupled

between the access router 60 and the end user systems 20. The DSLAMs 62 aggregate and forward DSL traffic from the end user systems 20 to the access router 60.

The access router 60 aggregates high capacity feeds from the DSLAMs 62. On the downstream side, the access router 60 receives multicast video streams from the transport network 16 or the satellite network 22 through the satellite receiver 28 and, as the last multicast router for the video streams, replicates multicast packets and forwarding them downstream. As described in more detail below, the access router 60 intercepts request for a user to join a multicast channel and authenticates the request using service selection gateway (SSG) 64. Accordingly, each access router 60 terminating point-to-point protocol (PPP) connections with the end user systems 20 should include an SSG image. The SSG 64 also allows a user to connect simultaneously to multiple destinations.

The end user systems 20 each include customer premise equipment (CPE) 70 and one or more host 72, which may be personal computers or other suitable computing devices. In a particular embodiment, the host 72 are PCs connected over an Ethernet local area network (LAN) with the CPE 70. The PCs include a web browser or other media player and/or plug-ins to display video data from a multicast stream. When the user starts a media player or plug-in to join a multicast channel, a join request is created for multicast channel and transmitted to the access network 18 for processing. In the IP embodiment, the join request is an IGMP join request. The PC is identified to the access network 18 based on its IP address.

In the communication system 10, the access router 60 in connection with the SSG 64, SSD server 42 and AAA server 44 provides a service architecture for video multicast services with support for authenticated access channels. Users log on to the network by connecting to a known uniform resource locator (URL) of the service provider of the access network 18 and then entering a login name and password on a login page. Successful log-ins display a dashboard menu of the users subscribed service packages. Users select a multicast package, which displays an associated web page that lists available channels or channel categories. When a user selects a channel, the channel is displayed in a viewer window in a web page. During login to the service provider and selection of a service package and/or channel, access privileges of the user are validated to allow service providers to completely control access to provided content.

FIGURE 2 illustrates details of the authentication components of the communications network 10 in accordance with one embodiment of the present invention. In this embodiment, authentication and other components of the communications system 10 may comprise logic encoded in media. The logic comprises functional instructions for carrying out the program task. The media comprises computer disk or other suitable computer-readable media, application specific integrated circuits (ASIC), field programmable gate arrays (FPGA), digital signal processor (DSP) or other suitable specific or general purpose processors, transmission media or other suitable media in which logic may be encoded and utilized.

Referring to FIGURE 2, the AAA server 44 comprises a RADIUS server 100 and a database 102. The RADIUS server 100 includes authentication and billing services for the service provider. Database 102 includes user profiles 104 and service profiles 106. The RADIUS server 100 communicates with SSG 64 and with the SSD server 42 using the RADIUS protocol. The SSD server 42 communicates with host 72 through the access router 60 using hypertext transfer protocol (HTTP). It will be understood that the servers router and host may communicate using other suitable protocols without departing from the scope of the present invention.

The access router 60 includes SSG 64 and a multicast routing table 110. SSG 64 includes a service profile 120 downloaded from database 102, a logged in table 122 and a multicast authentication engine 124. The service profile table 120 is maintained by and downloaded from the database 102. The service profile 120 contains a record of IP multicast ranges and service names for non-public multicast channels. Thus, public channels available to all users upon request are not listed in the service profile 120. The login table 122 maintains a record of all users currently logged in to the system and logged in to identified services.

The multicast authentication engine 124 intercepts multicast join request messages and authenticates whether the user is permitted to access the identified multicast channel using the service profile 120, login table 122 and/or the RADIUS server and database 100 and 102. Upon successful authentication, the multicast authentication engine 124 allows processing of the join request. Upon unsuccessful authentication, the multicast authentication

engine 124 discards, blocks or otherwise disallows the join request. Thus, the multicast stream is authenticated only at the join request. The actual multicast data packets need not be verified which minimizes authentication processing.

Multicast routing table 110 identifies users joined to each multicast channel. Accordingly, after successful authentication and processing of a join request, the user is added to the multicast routing table 110. Traffic received for a multicast channel is forwarded to each identified user. It will be understood that video channels may be provided to end users with or without modification by the access router 60.

In operation, to access a video service, users log in to the service provider network, select a multicast video service, and select a video channel. For user login, users connect through a web browser to a known address of the SSD server 42 and are presented with a user login page. Users enter a user name and password and the page is forwarded to the SSD server 42, which communicates with the RADIUS server 100 through SSG 64 to authenticate the user. The RADIUS server 100 accesses the database 102 and generates a RADIUS reply containing a list of services to which the user has subscribed. The SSD server 42 displays this list of services to the user via their browser in a dashboard menu format.

At service login, when the user selects a service from the dashboard, the selection is forwarded to the SSD server 42, which retrieves the service profile for the user from the RADIUS server 100. The SSD server 42 visually indicates to the user that the user is logged in to the service. The SSD server 42 then redirects the

browser to the proper URL which displays the service web page that contains a list of channels or channel categories for selection by the user. The logged in status of the user to the service provider and a service is recorded in the logged in table 122.

At channel access, when a user selects a channel, the users host device 72 issues an IGMP join request for the multicast channel through an interaction between a plug-in and media player. The plug-in learns the channel-to-IP address mapping by interacting with the web server associated with the service or by listening to a continuously multicast stream of mapping information. When the user joins a multicast channel by inclusion in the multicast routing table, the access router 60 forwards multicast packets to the user for display on the host screen.

Prior to processing of the IGMP join request, the SSG 64 intercepts the join message at the access router 60 and allows the join to succeed only if the channel is included in one of the services to which the user has currently logged in or the channel is a free channel as determined from the logged in table 122 and service profile 120. Because users can only log in to subscribed packages, user access is limited to only those channels included in their subscribed packages in addition to free channels.

In a specific embodiment, a host object is created in the logged in table 122 of SSG 64 when a user logs in to his or her account. When the user logs in to a service, SSG 64 creates a connection object and points to a service object for the user in the logged in table 122. Thus, if the user attempts to bypass normal procedures

and issues a join request through other means, multicast authentication will detect this by the absence of a valid connection object for the requested service and the join request will be dropped to prevent unauthorized access.

FIGURE 3 illustrates a method for authenticated access to multicast traffic in accordance with one embodiment of the present invention. The method begins at step 150 in which an IGMP or other suitable subscriber join request is received for a user to join a multicast channel providing content over a network.

Proceeding to decisional step 152, the access router 60 determines whether authentication is enabled. If authentication is not enabled, the No branch of decisional step 152 leads to step 154 in which the join request is allowed and processed. If authentication is enabled, the Yes branch of decisional step 152 leads to decisional step 158 for authentication.

At decisional step 158, the access router 60 determines whether the multicast channel is a public multicast channel to which all users are allowed access. If the multicast channel is public, the Yes branch of decisional step 158 also leads to step 154 in which the join request is allowed and processed. If the multicast channel is a non-public controlled access channel, such as a premium channel, the No branch of decisional step 158 leads to step 160.

At step 160, the user is determined based on the join request. In one embodiment, the SSG 64 translates between the host IP address and the user name and password to identify the user. User authentication may be based on user, device or other suitable identifier.

Next, at decisional step 162, the SSG 64 determines whether the user is logged in to the service provider. If the user is not logged in to the service provider, then the join request is improper and the No branch of decisional step 162 leads to step 164 in which the join request is disallowed. If the user is logged in to the service provider, the Yes branch of decisional step 162 leads to decisional step 166 for further authorization.

At step 166, the SSG 64 determines whether the user is logged in to a service including the multicast channel. Because login is only allowed to services for which the user has access privileges, determining that the user is logged in to the service validates that the user has access privileges to a service. It will be understood that access privileges of a user to a multicast channel may be otherwise suitably authenticated without departing from the scope of the present invention. For example, the user profile may be directly checked to determine access privileges of the user to the service. If the user is logged in to the service, the user has access privileges to the multicast channel and the Yes branch of decisional step 166 leads to step 154 in which the join request is allowed. If the user is not logged in to the service or does not have access privileges, the No branch of decisional step 166 leads to step 164 in which the join request is disallowed. Accordingly, users may only access multicast channels to which they have access privileges. In this way, service providers may provide subscription-based content using bandwidth-efficient IP multicast.

Although the present invention has been described with several embodiments, various changes and

modifications may be suggested to one skilled in the art. It is intended that the present invention encompass such changes and modifications as fall within the scope of the appended claims.